FORM PTO-1390 (REV. 5-93)	U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE	ATTORNEY'S DOCKET NUMBER 10191/1739

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

U.S. APPLICATION NO. (If known, see 37 CFR 1.5)
09/786824

INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE (04.09.99)	PRIORITY DATE(S) CLAIMED (09.09.98)
PCT/DE99/02811	4 September 1999	9 September 1998

TITLE OF INVENTION
A KEY VERIFICATION METHOD

APPLICANT(S) FOR DO/EO/US

STROHBECK, Walter

Applicant(s) herewith submit to the United States Designated/Elected Office (DO/EO/US) the following items and other information

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This is an express request to begin national examination procedures (35 U.S.C. 371(f)) immediately rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and PCT Articles 22 and 39(1).
4. ☒ A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.
5. ☒ A copy of the International Application as filed (35 U.S.C. 371(c)(2))
   a. ☐ is transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☒ has been transmitted by the International Bureau.
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US)
6. ☒ A translation of the International Application into English (35 U.S.C. 371(c)(2)).
7. ☒ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))
   a. ☐ are transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☐ have been transmitted by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☒ have not been made and will not be made.
8. ☐ A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
9. ☒ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)) (unsigned).
10. ☒ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11. to 16. below concern other document(s) or information included:

11. ☒ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. ☐ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. ☒ A **FIRST** preliminary amendment.
    ☐ A **SECOND** or **SUBSEQUENT** preliminary amendment.
14. ☒ A substitute specification and a marked up version of the substitute specification.
15. ☐ A change of power of attorney and/or address letter.
16. ☒ Other items or information: International Search Report, International Preliminary Examination Report, and Form PCT/RO/101.

Express Mail No. EL302703402

U.S. APPLICATION NO. if known, see 37 C.F.R.1.5	INTERNATIONAL APPLICATION NO.	ATTORNEY'S DOCKET NUMBER
09/786824	PCT/DE99/02811	10191/1739

17. ☒ The following fees are submitted:

	CALCULATIONS	PTO USE ONLY
Basic National Fee (37 CFR 1.492(a)(1)-(5)): Search Report has been prepared by the EPO or JPO $860.00		
International preliminary examination fee paid to USPTO (37 CFR 1.482) $690.00		
No international preliminary examination fee paid to USPTO (37 CFR 1.482) but international search fee paid to USPTO (37 CFR 1.445(a)(2)) $710.00		
Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO $1000.00		
International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(2)-(4) $100.00		
ENTER APPROPRIATE BASIC FEE AMOUNT =	$ 860	
Surcharge of $130.00 for furnishing the oath or declaration later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492(e)).	$	

Claims	Number Filed	Number Extra	Rate		
Total Claims	30 - 20 =	10	X $18.00	$ 180	
Independent Claims	5 - 3 =	2	X $80.00	$ 160	
Multiple dependent claim(s) (if applicable)			+ $270.00	$ 0	
TOTAL OF ABOVE CALCULATIONS =				$1,200	
Reduction by 1/2 for filing by small entity, if applicable. Verified Small Entity statement must also be filed. (Note 37 CFR 1.9, 1.27, 1.28).				$	
SUBTOTAL =				$1,200	
Processing fee of $130.00 for furnishing the English translation later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492(f)).			+	$	
TOTAL NATIONAL FEE =				$1,200	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). $40.00 per property			+	$	
TOTAL FEES ENCLOSED =				$1,200	
				Amount to be: refunded	$
				charged	$

a. ☐ A check in the amount of $_____ to cover the above fees is enclosed.

b. ☒ Please charge my Deposit Account No. 11-0600 in the amount of $1,200.00 to cover the above fees. A duplicate copy of this sheet is enclosed.

c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 11-0600. A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

Kenyon & Kenyon
One Broadway
New York, New York 10004

SIGNATURE

Richard L. Mayer, Reg. No. 22,490
NAME

3/9/2001
DATE

Reg. No. 33,865
Please Charge DK 01761

355502

26646
PATENT TRADEMARK OFFICE

[10191/1739]

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s)	:	Walter STROHBECK
Serial No.	:	To Be Assigned
Filed	:	Herewith
For	:	A KEY VERIFICATION METHOD
Art Unit	:	To Be Assigned
Examiner	:	To Be Assigned

Assistant Commissioner
for Patents
Washington, D.C. 20231

PRELIMINARY AMENDMENT AND
37 C.F.R. § 1.125 SUBSTITUTE SPECIFICATION STATEMENT

SIR:

Please amend the above-identified application before examination, as set forth below.

IN THE SPECIFICATION AND ABSTRACT:

In accordance with 37 C.F.R. § 1.121(b)(3), a Substitute Specification (including the Abstract, but without claims) accompanies this response. It is respectfully requested that the Substitute Specification (including Abstract) be entered to replace the Specification of record.

IN THE CLAIMS:

Without prejudice, please cancel original claims 1 to 29 and also cancel substitute claim 1, and please add new claims 30 to 59 as follows:

30. (New) A method for providing key verification for use with a security system, the security system including at least one valid key and an electronic verification arrangement having a transceiver for communicating with the at least one valid key, the electronic verification

arrangement storing unique identification data for the at least one valid key and storing enable data corresponding to the unique identification data for the at least one valid key, the electronic verification arrangement generating an authority for accessing a secured object when authentication data is received from the at least one valid key, the method comprising the steps of:

accessing the unique identification data for the at least one valid key in a mode of the security system;

performing a predetermined procedure to enter a key validation mode of the security system, the step of performing the predetermined procedure being performed by a user of the security system;

retaining enable data for each of the at least one valid key within a transceiver range in the key validation mode;

deleting other enable data for each of the at least one valid key outside the transceiver range in the key validation mode; and

deactivating each of the at least one key for which the other enable data is deleted in the step of deleting.

31. (New) The method of claim 30, wherein the predetermined procedure includes a vehicle starting procedure.

32. (New) The method of claim 30, wherein the predetermined procedure includes a vehicle access procedure.

33. (New) The method of claim 30, wherein the predetermined procedure includes a standard vehicle procedure using a standard vehicle control.

34. (New) The method of claim 33, wherein the standard vehicle control includes at least one of a brake pedal, a clutch pedal, an ignition switch, a start switch and a door handle.

35. (New) The method of claim 33, wherein:

the predetermined procedure includes at least one of a vehicle starting procedure and a vehicle access procedure; and

steps of the at least one of the vehicle starting procedure and the vehicle access procedure are performed at different times than times for performing the standard vehicle procedure.

36. (New) The method of claim 30, further comprising the step of indicating completion of the key validation mode.

37. (New) The method of claim 30, further comprising the step of generating a display of at least one activated valid key of the security system to indicate completion of the key validation mode.

38. (New) The method of claim 30, wherein the at least one key is without an activating button.

39. (New) The method of claim 30, wherein the enable data includes a control byte.

40. (New) The method of claim 30, wherein the authority allows access to the secured object.

41. (New) The method of claim 40, wherein the secured object is a vehicle.

42. (New) The method of claim 30, wherein the secured object is a vehicle and the authority allows operation of the vehicle.

43. (New) The method of claim 42, wherein the operation includes starting the vehicle.

44. (New) A security system comprising:

at least one valid key; and

an electronic verification arrangement including a transceiver for communicating with the at least one valid key and including a mode for accessing unique identification data, wherein the electronic verification arrangement is operable to:

store the unique identification data for the at least one valid key;

generate an authority for accessing a secured object when authentication data is received from the at least one valid key;

store enable data in accordance with the unique identification data for each activated one of the at least one valid key;

enter a key validation mode when a user performs a predetermined procedure;

retain enable data for each of the at least one valid key within a transceiver range in the key validation mode; and

delete other enable data for each of the at least one valid key outside the transceiver range in the key validation mode.

45. (New) The security system of claim 44, wherein the predetermined procedure includes a vehicle starting procedure.

46. (New) The security system of claim 44, wherein the predetermined procedure includes a vehicle entry procedure.

47. (New) The security system of claim 44, wherein the predetermined procedure includes a standard vehicle procedure using a standard vehicle control.

48. (New) The security system of claim 47, wherein the standard vehicle control includes at least one of a brake pedal, a clutch pedal, an ignition switch, a start switch and a door handle.

49. (New) The security system of claim 47, wherein:

the predetermined procedure includes at least one of a vehicle starting procedure and a vehicle entry procedure; and

steps of the at least one of the vehicle starting procedure and the vehicle entry procedure are performed at different times than times for performing the standard vehicle procedure.

50. (New) The security system of claim 44, further comprising an indicating arrangement for indicating completion of the key validation mode.

51. (New) The security system of claim 44, further comprising an indicating arrangement for generating a display of at least one activated valid key of the security system.

52. (New) The security system of claim 44, wherein the at least one key is without an activating button.

53. (New) The security system of claim 44, wherein the enable data includes a control byte.

54. (New) The security system of claim 44, wherein the authority allows access to the secured object.

55. (New) The security system of claim 54, wherein the secured object is a vehicle.

56. (New) The security system of claim 44, wherein the secured object is a vehicle and the authority allows operation of the vehicle.

57. (New) The security system of claim 56, wherein the operation includes starting the vehicle.

58. (New) A vehicle comprising:

a security system including:

at least one valid key; and

an electronic verification arrangement including a transceiver for communicating with the at least one valid key and including a mode for accessing unique identification data, wherein the electronic verification arrangement is operable to:

store the unique identification data for the at least one valid key;

generate an authority for accessing a secured object when authentication data is received from the at least one valid key;

store enable data in accordance with the unique identification data for each activated one of the at least one valid key;

enter a key validation mode when a user performs a predetermined procedure;

retain enable data for each of the at least one valid key within a transceiver range in the key validation mode; and

delete other enable data for each of the at least one valid key outside the transceiver range in the key validation mode.

59. (New) A security system for use with a motor vehicle, the security system comprising:

at least one key including an identification number; and

an electronic control unit including a transmitter/receiver for communicating with the at least one key and for receiving the identification number, and including a memory for storing identification data to provide stored identification data, the electronic control unit granting at least one of access and start-up operation of the motor vehicle if the identification number is included in the stored identification data of the memory;

wherein:

at least one enabling information message is storable in the memory and is associated with the identification number of the at least one key;

the electronic control unit in a validation mode causes each of the at least one key located within a broadcast range of the transmitter/receiver to transmit another identification number of each the at least one key located within the broadcast range, for setting the enabling information message of the another identification number of each the at least one key located within the broadcast range to provide a set enabling information message, and for resetting other enabling information of the at least one enabling information message for all other identification data stored in the memory; and

the electronic control unit grants at least one of access and driving authorization only in response to the set enabling information message.

REMARKS

This Preliminary Amendment cancels without prejudice original claims 1 to 29 and substitute claim 1 in the underlying PCT Application No. PCT/DE99/02811, and adds without prejudice new claims 30 to 59. The new claims conform the claims to U.S. Patent and Trademark Office rules and do not add new matter to the application.

In accordance with 37 C.F.R. § 1.121(b)(3), the Substitute Specification (including the Abstract, but without the claims) contains no new matter. The amendments reflected in the

Substitute Specification (including Abstract) are to conform the Specification and Abstract to U.S. Patent and Trademark Office rules or to correct informalities. As required by 37 C.F.R. § 1.121(b)(3)(iii) and § 1.125(b)(2), a Marked Up Version Of The Substitute Specification comparing the Specification of record and the Substitute Specification also accompanies this Preliminary Amendment. Approval and entry of the Substitute Specification (including Abstract) is respectfully requested.

The underlying PCT Application No. PCT/DE99/02811 includes an International Search Report, dated March 8, 2000. The Search Report includes a list of documents that were uncovered in the underlying PCT Application. A copy of the Search Report accompanies this Preliminary Amendment.

The underlying PCT application also includes an International Preliminary Examination Report, dated October 2, 2000, and an annex. An English translation of the International Preliminary Examination Report and the annex accompanies this Preliminary Amendment.

Applicant asserts that the subject matter of the present application is new, non-obvious, and useful. Prompt consideration and allowance of the application are respectfully requested.

Respectfully Submitted,
KENYON & KENYON

Dated: 3/9/2001

By: Richard Mayer
Richard L. Mayer
(Reg. No. 22,490)

Reg. No. 33,805
Aaron C. Dietz

One Broadway
New York, NY 10004
(212) 425-7200

354530v2

A KEY VERIFICATION METHOD

FIELD OF THE INVENTION

The present invention relates to a key verification method and a security system.

BACKGROUND INFORMATION

Passive security systems are available for vehicles which use remote keys having transponders that communicate with a transceiver of a vehicle, when the transponder is within range of the transceiver. Provided communication between a key and the transceiver follows a predetermined communications protocol, and unique authentication data is exchanged and validated, the key is considered a valid key and the system allows entry to and/or use of the vehicle. When the valid key subsequently moves out of range of the transceiver, the security system secures the vehicle by locking and immobilizing the vehicle.

When a valid key for a vehicle becomes lost, the key needs to be deactivated so it can no longer be used to gain access to the vehicle. Accordingly, it is desired to provide a simple technique for deactivating lost keys and reactivating found valid keys, particularly when the keys are buttonless.

SUMMARY OF THE INVENTION

In an exemplary embodiment of the present invention, there is

provided an exemplary key verification method for a security system including at least one valid key and an electronic control apparatus, arrangement or unit with a transceiver for communicating with the at least one valid key. The control apparatus, arrangement or unit generates an authority for access to a secured object when authentication data is received from the at least one valid key and storing unique identification data for the at least one valid key, this method including accessing the unique identification data for the at least one valid key in a mode of the system.

The exemplary method includes storing enable data corresponding to the unique identification data for the at least one valid key, a user executing a predetermined procedure to enter a key validation mode of the system, and in the validation mode retaining the enable data for valid keys within range of the transceiver and deleting the enable data for valid keys which are out of range of the transceiver, keys without the enable data being deactivated for the system.

The exemplary embodiment of the present invention also provides a security system including at least one valid key and electronic control apparatus, arrangement or unit with a transceiver for communicating with the at least one valid key, the control apparatus, arrangement or unit generating an authority for access to a secured object when authentication data is received from the at least one valid key and storing unique identification data for the at least one valid key, the system having a mode for accessing the unique identification data for the at least one valid key.

In an exemplary embodiment, the control apparatus, arrangement or unit stores enable data corresponding to the unique identification data for the at least one valid key when activated for the system, and the control apparatus, arrangement or unit enters a key validation mode when a user executes a predetermined procedure, and in the validation mode the enable data is retained for valid keys within range of the transceiver and deleted for valid keys out of range of the transceiver.

BRIEF DESCRIPTION OF THE DRAWING

Figure 1 is a block diagram of an exemplary embodiment of a security system.

DETAILED DESCRIPTION

A security system, as shown in Figure 1, includes an electronic control unit (ECU) 2, which is mounted in a vehicle and includes processing circuitry to communicate with other electrical and electronic components of the vehicle and the security system. In particular, ECU 2 includes an rf transceiver 14 for generating an rf signal which excites the transponder of a remote key 4 of the security system when key 4 is within the vicinity of a vehicle. Key 4 may have a card or fob. Once excited, key 4 uses rf transmission techniques to communicate with the transceiver, in accordance with a secure communications protocol, in order to pass authentication data from key 4 to ECU 2. Once received, ECU 2 compares the authentication data with security data that it holds in its memory, these being security codes and enable flags stored in an EEPROM 12. When ECU 2 finds a match between the received authentication data and its own security data, ECU 2 issues

signals to other components of the vehicle to enable access to and/or operation of the vehicle by the holder of key 4. When key 4 is removed from the immediate vicinity of the vehicle, this is detected by transceiver 14, which causes ECU 2 to generate signals to secure the vehicle, for example by locking and immobilizing the vehicle.

Normally, a number of valid keys can be used with the security system to gain access to the vehicle. Keys 4 each include a unique serial or identification number and this is communicated to ECU 2 as part of the authentication data. ECU 2 stores the serial numbers for each valid key in its EEPROM 12, and an enable flag is stored against each serial number. As an alternative to the enable flag, the system can store a control byte which may be an encoded version of the identification number. During the authentication procedure when ECU 2 verifies the authentication data, ECU 2 checks to determine whether the received serial number of the communicating key 4 is stored in EEPROM 12 and whether its enable flag is set or reset. If the serial number is found and the enable flag is set, then the communicating key constitutes a valid key which can be used to gain access to the vehicle. If however the serial number is found and the enable flag is not set, then the communicating key is no longer a valid key which can be used. The ECU 2 is capable of deactivating the key and carrying out an activation procedure which resets and sets the enable flag for key 4. This enables a vehicle owner whose keys have been lost or stolen to proceed in a simple manner as described above.

If a valid key has been lost or stolen, the holder of at least

one remaining valid key can set ECU 2 to a key validation mode in order to validate all the remaining keys. The holder of the remaining keys simply enters the vehicle, brings all the remaining keys within range of transceiver 14, and executes a predetermined procedure to put ECU 2 into the key validation mode. When ECU 2 is in the key validation mode, ECU 2 turns on all the keys 4 within its range in order to receive their serial numbers and sets the enable flags in EEPROM 12 for the received serial numbers, while the enable flags for all the other key serial numbers stored in EEPROM 12 are reset. The keys within range of transceiver 14 will then represent valid keys and the lost or stolen key will no longer be a valid key, since its enable flag is reset. The ECU 2 displays the completion of the key validation procedure by generating a completion signal for a message unit 6. The message unit simply shows either visually or acoustically that the key validation procedure has been completed. Message unit 6 may be an LED in the vehicle or a horn or a siren of the vehicle. Message unit 6 may also be a display unit in the vehicle, which receives the data and is capable of showing which keys are valid for the vehicle. The display unit could also display other messages, such as, for example "Key validation completed," and may include controls allowing a user of the vehicle to recall a display showing the valid keys, for example, key A, B, and C.

If the lost or stolen key 4 is recovered, the key can be revalidated or reactivated by bringing all the keys into the vehicle again and placing ECU 2 in the key validation mode in order to execute the above-explained key validation procedure. The enable flag for the found key 4 will then be set in EEPROM

To avoid the requirement for any additional hardware components to be added to the vehicle, the predetermined procedure used to place ECU 2 in the key validation mode needs to be executed (or performed) using existing (or standard) vehicle components. The predetermined procedure should advantageously involve using components and operations which are normally involved in a start or entry procedure for the vehicle. Vehicles may have a start procedure which involves pressing a pedal 8, which may be the brake or clutch pedal, and then simultaneously turning on an ignition start switch 10 of the vehicle. The ECU 2 is connected to the electric network or wiring harness of the vehicle so as to receive signals generated when pedal 8 is depressed and ignition start switch 10 is turned on. The predetermined procedure to enter the key validation mode can then involve the holder of the keys simply depressing pedal 8 and turning on ignition start switch 10 alternately a number of times, say three times, instead of doing this simultaneously. The ECU 2 on detecting depression of pedal 8 and turning on of ignition start switch 10 alternately can then generate a message for message unit 6 to confirm entry into the key validation mode when the predetermined procedure has been executed. The ECU 2 can also issue cues on message unit 6 to follow the time sequence for depression of pedal 8 and turning on ignition start switch 10, to assist the holder of the keys in correctly executing the procedure to enter the key validation mode. Alternatively, the steps and vehicle components used for entry into the vehicle can be used; for example, in some passive security systems the key is excited on lifting a door handle 16. The

predetermined procedure required to enter the key validation mode may require a holder of the keys to lift door handle 16 a number of times within a certain period of time, for example four times in two seconds.

The ECU 2 can be provided by or divided into a number of ECUs, and similarly the vehicle can include a number of transceivers and antennas to communicate with remote keys 4. Keys 4 may be passive entry keys which require energy from the vehicle in order to communicate with ECU 2 or the keys may have their own battery power supply. Also, while the exemplary methods and embodiments of the present inventions are believed to be particularly advantageous for keys which have no activating buttons, keys 4 can include activating buttons and the security system may be a combination of active and passive security systems. For example, the security system may be designed such that key 4 is able to communicate over a distance, of for example 30 m, with the vehicle when activated, and is also able to be energized or excited when closer to the vehicle by, for example, lifting the door handle, or some other activation device, when in the vicinity of the vehicle.

ABSTRACT OF THE DISCLOSURE

A key verification method for a security system, which includes one valid key and an electronic verification control with a transceiver for communicating with the valid key, includes using the electronic verification control for generating an authority for access to a secured object when authentication data is received from the valid key and storing unique identification data for the valid key, accessing the unique identification data for the valid key in one mode of the system by storing enable data corresponding to the unique identification data for the valid key, executing or performing a predetermined procedure to enter a key validation mode of the system, and, in the validation mode, retaining the enable data for valid keys within range of the transceiver and deleting the enable data for valid keys which are out of range of the transceiver, and deactivating keys without the enable data for the system. Also described is a security system including one valid key and an electronic verification control with a transceiver for communicating with the valid key, in which the electronic verification control includes a mode for accessing the unique identification data for the valid key, and generating an authority for access to a secured object when authentication data is received from the valid key and storing unique identification data for the valid key enabling data corresponding to the unique identification data for the valid key when activated for the system, entering a key validation mode when a user executes a predetermined procedure, and, in the validation mode, retaining the enable data for valid keys within range of the transceiver and deleting it for valid keys out of range of the transceiver.

353922

1/PRTS

A KEY VERIFICATION METHOD

The present invention relates to a key verification method and a security system.

Passive security systems are available for vehicles which use remote keys having transponders that communicate with a transceiver of a vehicle, when the transponder is within range of the transceiver. Provided communication between a key and the transceiver follows a predetermined communications protocol, and unique authentication data is exchanged and validated, the key is considered a valid key and the system allows entry to and/or use of the vehicle. When the valid key subsequently moves out of range of the transceiver, the security system secures the vehicle by locking and immobilizing the vehicle.

When a valid key for a vehicle becomes lost, the key needs to be deactivated so it can no longer be used to gain access to the vehicle. Accordingly, it is desired to provide a simple technique for deactivating lost keys and reactivating found valid keys, particularly when the keys are buttonless.

In accordance with the present invention, there is provided a key verification method for a security system including at least one valid key and electronic control means with a transceiver for communicating with the at least one valid key, the control means generating an authority for access to a

secured object when authentication data is received from the at least one valid key and storing unique identification data for the at least one valid key, this method including accessing the unique identification data for the at least one valid key in a mode of the system;

characterized by storing enable data corresponding to the unique identification data for the at least one valid key, a user executing a predetermined procedure to enter a key validation mode of the system, and in the validation mode retaining the enable data for valid keys within range of the transceiver and deleting the enable data for valid keys which are out of range of the transceiver, keys without the enable data being deactivated for the system.

The present invention also provides a security system including at least one valid key and electronic control means with a transceiver for communicating with the at least one valid key, the control means generating an authority for access to a secured object when authentication data is received from the at least one valid key and storing unique identification data for the at least one valid key, the method having a mode for accessing the unique identification data for the at least one valid key;

characterized in that the control means stores enable data corresponding to the unique identification data for the at least one valid key when activated for the system, and the control means enters a key validation mode when a user executes a predetermined procedure, and in the validation mode the enable data is retained for valid keys within range of the transceiver and deleted for valid keys out of range of the

transceiver.

A preferred embodiment of the present invention is hereinafter described, by way of example, with reference to the accompanying drawing, wherein:

Figure 1 is a block diagram of a preferred embodiment of a security system.

A security system, as shown in Figure 1, includes an electronic control unit (ECU) 2, which is mounted in a vehicle and includes processing circuitry to communicate with other electrical and electronic components of the vehicle and the security system. In particular, ECU 2 includes an rf transceiver 14 for generating an rf signal which excites the transponder of a remote key 4 of the security system when key 4 is within the vicinity of a vehicle. Key 4 may have a card or fob. Once excited, key 4 uses rf transmission techniques to communicate with the transceiver, in accordance with a secure communications protocol, in order to pass authentication data from key 4 to ECU 2. Once received, ECU 2 compares the authentication data with security data that it holds in its memory, these being security codes and enable flags stored in an EEPROM 12. When ECU 2 finds a match between the received authentication data and its own security data, ECU 2 issues signals to other components of the vehicle to enable access to and/or operation of the vehicle by the holder of key 4. When key 4 is removed from the immediate vicinity of the vehicle, this is detected by transceiver 14, which causes ECU 2 to generate signals to secure the vehicle, for example by locking and immobilizing the vehicle.

Normally, a number of valid keys can be used with the security system to gain access to the vehicle. Keys 4 each include a unique serial or identification number and this is communicated to ECU 2 as part of the authentication data. ECU 2 stores the serial numbers for each valid key in its EEPROM 12, and an enable flag is stored against each serial number. As an alternative to the enable flag, the system can store a control byte which may be an encoded version of the identification number. During the authentication procedure when ECU 2 verifies the authentication data, ECU 2 checks to determine whether the received serial number of the communicating key 4 is stored in EEPROM 12 and whether its enable flag is set or reset. If the serial number is found and the enable flag is set, then the communicating key constitutes a valid key which can be used to gain access to the vehicle. If however the serial number is found and the enable flag is not set, then the communicating key is no longer a valid key which can be used. ECU 2 is capable of deactivating the key and carrying out an activation procedure which resets and sets the enable flag for key 4. This enables a vehicle owner whose keys have been lost or stolen to proceed in a simple manner as described above.

If a valid key has been lost or stolen, the holder of at least one remaining valid key can set ECU 2 to a key validation mode in order to validate all the remaining keys. The holder of the remaining keys simply enters the vehicle, brings all the remaining keys within range of transceiver 14, and executes a predetermined procedure to put ECU 2 into the key validation mode. When ECU 2 is in the key validation mode, ECU 2 turns on all the keys 4 within its range in order to receive their serial numbers and sets the enable flags in EEPROM 12 for the

received serial numbers, while the enable flags for all the other key serial numbers stored in EEPROM 12 are reset. The keys within range of transceiver 14 will then represent valid keys and the lost or stolen key will no longer be a valid key, since its enable flag is reset. ECU 2 displays the completion of the key validation procedure by generating a completion signal for a message unit 6. The message unit simply shows either visually or acoustically that the key validation procedure has been completed. Message unit 6 may be an LED in the vehicle or a horn or a siren of the vehicle. Message unit 6 may also be a display unit in the vehicle, which receives the data and is capable of showing which keys are valid for the vehicle. The display unit could also display other messages, such as, for example "Key validation completed," and may include controls allowing a user of the vehicle to recall a display showing the valid keys, for example, key A, B, and C.

If the lost or stolen key 4 is recovered, the key can be revalidated or reactivated by bringing all the keys into the vehicle again and placing ECU 2 in the key validation mode in order to execute the above-explained key validation procedure. The enable flag for the found key 4 will then be set in EEPROM 12.

To avoid the requirement for any additional hardware components to be added to the vehicle, the predetermined procedure used to place ECU 2 in the key validation mode needs to be executed using existing vehicle components. The predetermined procedure should advantageously involve using components and operations which are normally involved in a start or entry procedure for the vehicle. Most vehicles have a

start procedure which involves pressing a pedal 8, which may be the brake or clutch pedal, and then simultaneously turning on an ignition start switch 10 of the vehicle. ECU 2 is connected to the electric network or wiring harness of the vehicle so as to receive signals generated when pedal 8 is depressed and ignition start switch 10 is turned on. The predetermined procedure to enter the key validation mode can then involve the holder of the keys simply depressing pedal 8 and turning on ignition start switch 8 alternately a number of times, say three times, instead of doing this simultaneously. ECU 2 on detecting depression of pedal 8 and turning on of ignition start switch 10 alternately can then generate a message for message unit 6 to confirm entry into the key validation mode when the predetermined procedure has been executed. ECU 2 can also issue cues on message unit 6 to follow the time sequence for depression of pedal 8 and turning on ignition start switch 8, to assist the holder of the keys in correctly executing the procedure to enter the key validation mode. Alternatively the steps and vehicle components used for entry into the vehicle can be used - for example, in some passive security systems the key is excited on lifting a door handle 16. The predetermined procedure required to enter the key validation mode may require a holder of the keys to lift door handle 16 a number of times within a certain period of time, for example four times in two seconds.

ECU 2 can be provided by or divided into a number of ECUs, and similarly the vehicle can include a number of transceivers and antennas to communicate with remote keys 4. Keys 4 may be passive entry keys which require energy from the vehicle in order to communicate with ECU 2 or the keys may have their own battery power supply. Also, whilst the present invention is

particularly advantageous for keys which have no activating buttons, keys 4 can include activating buttons and the security system may be a combination of active and passive security systems. For example, the security system may be designed such that key 4 is able to communicate over a distance, of for example 30 m, with the vehicle when activated, and is also able to be energized or excited when closer to the vehicle by, for example, lifting the door handle, or some other activation device, when in the vicinity of the vehicle.

Many modifications will be apparent to those skilled in the art without departing from the scope of the present invention as herein described with reference to the accompanying drawings.

What is claimed is:

1. A key verification method for a security system including at least one valid key and electronic verification means having a transceiver for communicating with the at least one valid key, the verification means generating an authority for access to a secured object when authentication data is received from the at least one valid key, and storing unique identification data for the at least one valid key, the method including accessing the unique identification data for the at least one valid key in a mode of the system;
characterized in that enable data corresponding to the unique identification data for the at least one valid key are stored, a user executing a predetermined procedure to enter a key validation mode of the system and, in the validation mode, to retain the enable data for valid keys within range of the transceiver, and delete the enable data for valid keys which are out of range of the transceiver, keys without the enable data being deactivated for the system.

2. The key verification method according to Claim 1, wherein the predetermined method includes steps of the start procedure of a vehicle.

3. The key verification method according to Claim 1, wherein the predetermined method includes steps of an access procedure to a vehicle.

4. The key verification method according to Claim 1, wherein the predetermined method includes executing steps using standard controls of a vehicle.

5. The key verification method according to Claim 4, wherein the standard controls include a brake pedal, a clutch pedal, an ignition start switch, and/or a door handle.

6. The key verification method according to one of Claims 2 through 5, wherein the steps are executed at times relative to one another which differ from the times for the standard procedures for the vehicle.

7. The key verification method according to one of the preceding claims, including completion of the key validation mode.

8. The key verification method according to Claim 7, wherein the indicating includes generating a display of the activated valid keys for the system.

9. The key verification method according to one of the preceding claims, wherein the keys are without activating buttons.

10. The key verification method according to one of the preceding claims, wherein the enable data is a control byte.

11. The key verification method according to one of Claims 1 to 10, wherein the authority allows access to the secured object.

12. The key verification method according to Claim 11, wherein the secured object is a vehicle.

13. The key verification method according to one of Claims 1

to 10, wherein the secured object is a vehicle and the authority allows operation of the vehicle.

14. The key verification method according to Claim 13, wherein the operation includes starting the vehicle.

15. A security system comprising at least one valid key and electronic verification means having a transceiver for communicating with the at least one valid key, the verification means generating an authority for access to a secured object when authentication data is received from the at least one valid key, and storing unique identification data for the at least one valid key, the method having a mode for accessing the unique identification data for the at least one valid key, characterized in that the verification means stores enable data in accordance with the unique identification data for the at least one valid key when they are activated for the system, and that the verification means enters a key validation mode when a user executes a predetermined method and, in the validation mode, the enable data is retained for valid keys within range of the transceiver and deleted for valid keys out of range of the transceiver.

16. The security system according to Claim 15, wherein the predetermined method includes steps of a start procedure of a vehicle.

17. The security system according to Claim 15, wherein the predetermined method includes steps of an entry procedure into a vehicle.

18. The security system according to Claim 15, wherein the

predetermined method includes executing steps using standard controls of a vehicle.

19. The security system according to Claim 18, wherein the standard controls include a brake pedal, a clutch pedal, an ignition switch, and/or a door handle.

20. The security system according to one of Claims 16 to 19, wherein the steps are executed at times relative to one another, which differ from the times for the standard procedures for the vehicle.

21. The security system according to one of Claims 15 to 20, including means for indicating completion of the key validation mode.

22. The security system according to Claim 21, wherein the indicating means include the display of the current valid keys for the system.

23. The security system according to one of Claims 15 to 22, wherein the keys are without activating buttons.

24. The security system according to one of Claims 15 to 23, wherein the enable data are a control byte.

25. The security system according to one of Claims 15 to 24, wherein the authority allows access to the secured object.

26. The security system according to Claim 25, wherein the secured object is a vehicle.

27. The security system according to one of Claims 15 to 24, wherein the secured object is a vehicle and the authority allows operation of the vehicle.

28. The security system according to Claim 27, wherein the operation includes starting the vehicle.

29. A vehicle comprising a security system according to one of Claims 15 to 28.

Abstract

A key verification method is described for a security system including at least one valid key and electronic verification means with a transceiver for communicating with the at least one valid key, the verification means generating an authority for access to a secured object when authentication data is received from the at least one valid key and storing unique identification data for the at least one valid key, the method including accessing the unique identification data for the at least one valid key in one mode of the system, characterized by storing enable data corresponding to the unique identification data for the at least one valid key, a user executing a predetermined procedure to enter a key validation mode of the system, and in the validation mode retaining the enable data for valid keys within range of the transceiver and deleting the enable data for valid keys which are out of range of the transceiver, keys without the enable data being deactivated for the system.

A security system including at least one valid key and electronic verification means with a transceiver for communicating with the at least one valid key, the verification means generating an authority for access to a secured object when authentication data is received from the at least one valid key and storing unique identification data for the at least one valid key, the method having a mode for accessing the unique identification data for the at least one valid key, characterized in that the verification means stores enable data corresponding to the unique identification data for the at least one valid key when activated for the system, and the verification means enters a key validation mode when a

user executes a predetermined procedure, and in the validation mode the enable data is retained for valid keys within range of the transceiver and deleted for valid keys out of range of the transceiver.

353901v1

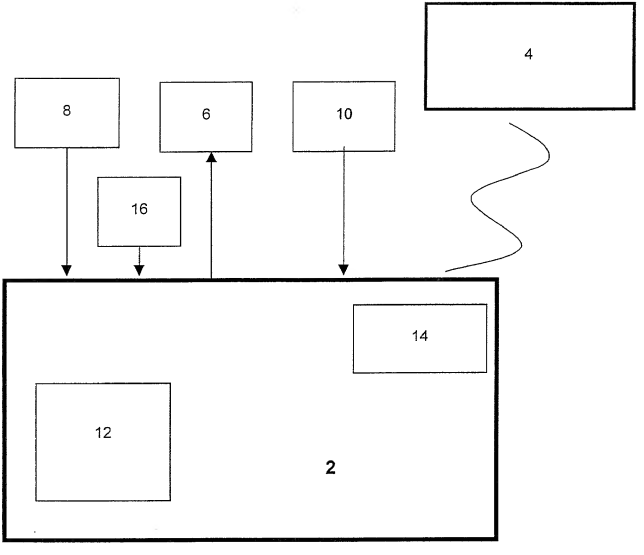

Figure 1

DECLARATION AND POWER OF ATTORNEY

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled **A KEY VERIFICATION METHOD**, the specification of which was filed as International Application No. **PCT/DE99/02811** on September 4, 1999.

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, § 1.56(a).

I hereby claim foreign priority benefits under Title 35, United States Code, § 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application(s) for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

EL244503996
~~EL302703402~~

PRIOR FOREIGN APPLICATION(S)

Number	Country filed	Day/month/year	Priority Claimed Under 35 USC 119
PP5763	Australia	9 September 1998	Yes
43414/99	Australia	5 August 1999	Yes

And I hereby appoint Richard L. Mayer (Reg. No. 22,490) and Gerard A. Messina (Reg. No. 35,952) my attorneys with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith.

Please address all communications regarding this application to:

KENYON & KENYON
One Broadway
New York, New York 10004

Please direct all telephone calls to Richard L. Mayer at (212) 425-7200.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful and false statements may jeopardize the validity of the application or any patent issued thereon.

Inventor: **Walter STROHBECK**

Inventor's Signature: Walter Strohbeck

Date: 2 May 2001

Residence: 11 Mack Rd.
Narre Warren 3805
Australia AUS

Citizenship: Federal Republic of Germany

Post Office Address: Same as above.

355455